1. Objetivo general

Establecer lineamientos para la administración de contraseñas de los usuarios y administradores de las tecnologías de la información en la Secretaría Distrital de Integración Social - SDIS para mantener la triada de la Información. (Confidencialidad, Integridad y Disponibilidad).

2. Objetivos Específicos

- Crear buenas prácticas para la correcta administración de las contraseñas de las tecnologías de la Información en la SDIS.
- Cumplir con las políticas de Seguridad de la Información establecidas para uso de contraseñas en la SDIS.
- Evitar la materialización de riesgos de Seguridad de la Información por contraseñas inseguras o préstamos de las mismas.

3. Alcance

Aplica para todos los usuarios a quienes se les haya concedido permisos sobre los sistemas de información, bases de datos o servicios de tecnología, cualquiera que sea la función que desempeñen los funcionarios y contratistas de la SDIS.

4. Vigencia

El lineamiento tiene vigencia hasta que surtan modificaciones al mismo por cambios de Políticas de Seguridad o estructura del mismo.

5. Marco Conceptual

Active directory lightweight directory services: es un servicio de directorio del Protocolo Ligero de Acceso a Directorios (LDAP) del Sistema Operativo Windows Server® 2008 R2 que ofrece una compatibilidad flexible para aplicaciones habilitadas para el uso de directorios activos[1].

Aplicación: es un programa informático diseñado como herramienta con el fin de permitir a un usuario realizar uno o varios tipos de tareas.

[1] https://technet.microsoft.com/es-es/library/cc733064(v=ws.11).aspx

Autenticación: asegurar que una característica declarada de una entidad es correcta.[2]

Base de datos: es una colección de información organizada con el propósito que sea fácilmente accesible, administrada y actualizada.

Caja de seguridad: compartimiento de seguridad que ha sido inventado para que su apertura sea muy difícil para personas no autorizadas y así poder guardar elementos de valor, constan de un sistema de cierre que solo se puede abrir mediante claves secretas, y estas claves pueden cambiarse para preservar más aún la seguridad.[3]

Controlador de dominio: es una entidad administrativa que tiene una serie de responsabilidades, como es la autenticación, para garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, a través del uso de una contraseña.

Data center: se denomina también centro de procesamiento de datos (CPD) a aquella ubicación o espacio principal donde se concentran los recursos tecnológicos necesarios para el procesamiento de la información de una organización.

Directorio activo: centro de administración donde se almacena, mantiene y gestiona la base de datos de usuarios y recursos de la red.

Gestor de base de datos: es el conjunto de programas que administran y gestionan la información contenida en una base de datos.

Infraestructura tecnológica: es el conjunto de hardware y software empleados para optimizar la productividad y el funcionamiento de los diferentes servicios de la SDIS.

Root: es un usuario privilegiado, que cuenta con control absoluto de acceso a todas las funciones de un sistema.

Servicio tecnológico: es un conjunto de actividades que buscan responder a las necesidades de un usuario por medio de un conjunto tecnológico.

6. Justificación

Este lineamiento respalda la Política de Seguridad de la Información – Resolución 0635 del 12 de abril de 2017.

7. Antecedentes

La Subdirección de Información y Tecnología en cumplimiento de la Política de Seguridad de la Información, ve la necesidad de implementar dicho lineamiento, teniendo en cuenta que al realizar

[2]Norma Técnica Colombiana NTC-ISO-IEC 27000

[3]http://micajayauditoria.blogspot.com.co/2011/04/guia-n-001-actividad-7-cierre-de.html

revisiones por parte del Subsistema de Seguridad de la Información se evidencia que los usuarios no están administrando de manera correcta sus contraseñas por lo cual puede presentarse incidentes de Seguridad de la Información.

8. Normatividad

- Resolución 0635 de 12 de abril de 2017 “Por el cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social”.

9. Principios

Todas las contraseñas de los usuarios de los servicios tecnológicos (acceso al equipo de cómputo, correo electrónico, sistemas de información: SIRBE, HEFI, IOPS, SIBI, etc.) de la SDIS deben cumplir las siguientes directrices:

- La Subdirección de Investigación e Información entregará a los usuarios las contraseñas respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados.

- Las contraseñas son de uso personal e intransferible, siendo responsables los funcionarios, contratistas y terceras partes el manejo que se les dé a las claves asignadas.

- Todas las contraseñas debe tener una longitud mínima de ocho (8) caracteres que debe cumplir con las siguientes características: incluir combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales (por ejemplo: (!,@,#, $,%,^,&,*,(),_, etc.) y ser cambiadas máximo cada cuarenta y cinco (45) días.

- Después de tres (3) intentos de acceso fallidos de manera consecutiva por ingreso de usuario y/o contraseña errados, el usuario será bloqueado hasta nueva reactivación por parte de la mesa de servicios.

10. Áreas o ejes temáticos del lineamiento o política interna

Política de Seguridad de la Información – Resolución 0635 del 12 de abril de 2017.

Contraseñas de usuarios administradores de la infraestructura tecnológica

Las siguientes directrices van dirigidas específicamente a aquellos que administran o son responsables de algún(os) servidor(es)y/o servicio(s)de la SDIS:

- Se requiere una autenticación centralizada a nivel directorio activo donde los administradores de servidores, aplicaciones, bases de datos o servicios tecnológicos, tenga un único usuario de autenticación, comprendidos de la siguiente manera:

- Usuarios administradores de servidores: son los usuarios que administran los controladores de dominio y/o servidores que se encuentren localizados en el data center; este usuario tendrá los privilegios más elevados en el manejo de la infraestructura tecnológica, ya que podrán realizar las siguientes acciones: crear, modificar, cambiar, aplicar y/o eliminar procesos dentro de los servidores. Para este tipo de usuario su contraseña debe ser cambiada cada tres (3) meses, entregándose esta contraseña en sobre sellado al líder del equipo de infraestructura.

- Usuarios administradores de aplicaciones: son los usuarios que tienen la capacidad de realizar parametrizaciones en las aplicaciones, así como ejecutar tareas específicas de eliminación y edición de información que, por la naturaleza de la misma, debe realizarse con autorización expresa del supervisor de contrato y/o jefe inmediato. Para este tipo de usuario y cuya autenticación se realiza contra el directorio activo, la contraseña debe ser cambiada máxima cada cuarenta y cinco (45) días, para el caso de los usuarios propios de la aplicación, es decir, que no dependen del directorio activo, la contraseña debe ser cambiada cada tres (3) meses y las aplicaciones construidas por el equipo de desarrollo deben incluir la política que permita solicitar dicho cambio.

- Usuarios administradores de bases de datos: son los usuarios que administran desde los servidores, de los diferentes ambientes (pruebas y producción), las bases de datos de los aplicativos de la SDIS, este usuario tendrá los privilegios más elevados en el manejo de la información, actualización, disponibilidad y seguridad de la misma para la prestación de cada uno de los servicios sociales a los usuarios. Estos usuarios son súper administradores de las bases de datos, por lo cual tienen total control sobre estas, para este tipo de usuario su contraseña debe ser cambiada cada tres (3) meses por parte del administrador de base de datos, entregándose esta contraseña en sobre sellado al líder del equipo de infraestructura.

- Usuarios de la mesa de servicio: son los usuarios agentes mesa de servicio y/o soporte en sitio quienes brindarán servicios de solución a solicitudes, incidentes y gestión de cambios a los usuarios de la SDIS, estos usuarios tendrán sus respectivos privilegios. Los agentes mesa de servicio tendrán usuarios con privilegios elevados para el manejo del controlador del domino, pero, solo tendrán la opción de crear, modificar, reestablecer y/o deshabilitar cuentas, no podrán ingresar sobre los controladores de dominio ya que tendrían administración total sobre las políticas de directorio activo de la SDIS, se debe crear en cada equipo de los agentes, las consolas de conexión al directorio activo, tal característica se basa en active Directory Lightweight Directory Services. Las contraseñas deben ser cambiadas máximas cada cuarenta y cinco (45) días.

Las personas que realizan soporte técnico en sitio tendrán usuario de privilegios elevados como son los de administrador local sobre las máquinas de la entidad, ya que ellos necesitan en sus actividades instalar, configurar, desinstalar y/o colocar máquinas en el domino; estos usuarios como son de criticidad alta es necesario realizar el cambio de la contraseña cada dos (2) meses, esta actividad se realiza con la supervisión del administrador del dominio de la SDIS.

Custodia de contraseñas de servicios

Los líderes de equipo deben consolidar y entregar todas las contraseñas de administración de servidores, aplicaciones y servicios tecnológicos dentro de un sobre sellado y firmado por el custodio de las mismas, este sobre se debe encontrar bajo llave a responsabilidad del Subdirector (a) de la Subdirección de Investigación e Información y se deben cambiar semestralmente destruyendo en totalidad los anteriores.

Todo cambio de estas claves debe ser informado al Subdirector (a) y actualizado en los respectivos sobres sellados en la caja de seguridad.

11. Evaluación del lineamiento o política interna

La evaluación del lineamiento se realizará a través de encuestas diseñadas para medir la percepción y adopción del Subsistema de Gestión de Seguridad de la Información en la SDIS.

12. Responsabilidades y competencias

Los responsables de ejecutar este lineamiento son todos los usuarios que hacen parte de la SDIS.

13. Administración del lineamiento

Dirección de Análisis y Diseño Estratégico - Subdirección de Investigación e Información

14. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	Dayana Carbonó Carbonó	Jennifer Patricia Duran Vargas Katheryn Gonzalez Castillo Rocío Gómez Rodríguez	Liliana Pulido Villamil
Cargo/ Rol	Contratista- SII Seguridad de la información	Contratista – SII Gestor proceso y dependencia Contratista- SII Gestor Seguridad de la Información Contratista- SII Líder infraestructura Subdirectora Investigación e Información	Directora de Análisis y Diseño Estratégico